IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application for:

DECRYPTION SYSTEM

Inventor(s): Kim Annon Ryal

Docket Number: SNY-T5501.01

Prepared By: Miller Patent Services
2500 Dockery Lane
Raleigh, NC 27606

Phone: (919) 816-9981
Fax: (919) 816-9982
Email: miller@patent-inventions.com

CERTIFICATE OF EXPRESS MAILING FOR NEW PATENT APPLICATION

"Express Mail" mailing label number ER126259078US

Date of Deposit 9/15/2003

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450.

Catherine N. Miller

(Typed or printed name of person mailing paper or fee)

Catherine N. Miller

(Signature of person mailing paper or fee)

DECRYPTION SYSTEM

CROSS REFERENCE TO RELATED DOCUMENTS

This application is related to the following copending patent applications which are hereby incorporated herein by reference:

S/N 10/038,217 filed January 2, 2002,
S/N 10/038,032 filed January 2, 2002,
S/N 10/037,914 filed January 2, 2002,
S/N 10/037,499 filed January 2, 2002,
S/N 10/037,498 filed January 2, 2002,
S/N 10/084,106 filed February 2, 2002,
S/N 10/273,905 filed October 18, 2002,
S/N 10/273,903 filed October 18, 2002,
S/N 10/273,875 filed October 18, 2002,
S/N 10/274,084 filed October 18, 2002,
S/N 10/273,904 filed October 18, 2002,
S/N 10/274,019 filed October 18, 2002,
S/N 10/293,761 filed November 13, 2002,
S/N 10/303,594 filed November 25, 2002,
S/N 10/319,133 filed December 13, 2002,
S/N 10/319,066 filed December 13, 2002,
S/N 10/318,782 filed December 13, 2002,
S/N 10/319,169 filed December 13, 2002,
S/N 10/391,940 filed March 19, 2003,
S/N 10/393,324 filed March 20, 2003.

COPYRIGHT NOTICE

BACKGROUND

Selective encryption systems, including but not limited to dual or multiple selective encryption systems are disclosed in the above-referenced patent applications. Such systems are useful in providing encryption of program material under multiple conditional access systems.

The above-referenced commonly owned patent applications describe inventions relating to various aspects of methods generally referred to herein as partial encryption or selective encryption. More particularly, systems are described therein wherein selected portions of a particular selection of digital content are encrypted using two (or more) encryption techniques while other portions of the content are left unencrypted. By properly selecting the portions to be encrypted, the content can effectively be encrypted for use under multiple decryption systems without the necessity of encryption of the entire selection of content. In some embodiments, only a few percent of data overhead is needed to effectively encrypt the content using multiple encryption systems. This results in a cable or satellite system being able to utilize Set-top boxes or other implementations of conditional access (CA) receivers from multiple manufacturers in a single system - thus freeing the cable or satellite company to competitively shop for providers of Set-top boxes.

BRIEF DESCRIPTION OF THE DRAWINGS

Certain illustrative embodiments of the invention illustrating organization and method of operation, together with objects and advantages thereof, may be best

understood by reference detailed description that follows taken in conjunction with the accompanying drawings in which:

FIGURE 1 is a diagram depicting a dual selectively encrypted data stream consistent with certain embodiments of the present invention.

FIGURE 2 is a block diagram of a decoding system consistent with certain embodiments of the present invention.

FIGURE 3 is a drawing depicting another embodiment of a dual selectively encrypted data stream consistent with certain embodiments of the present invention.

FIGURE 4 is a block diagram of another embodiment of a decoding system consistent with certain embodiments of the present invention.

FIGURE 5 is another embodiment of a decoder system consistent with certain embodiments of the present invention.

FIGURE 6 is a block diagram of a system for generating a stream or file of clear packets in a manner consistent with certain embodiments of the present invention.

FIGURE 7 is a diagram showing another arrangement of clear packets that can be used in certain embodiments consistent with of the present invention.

FIGURE 8 is a flow chart of a decoding method consistent with certain embodiments of the present invention.

FIGURE 9 is a flow chart of a clear packet generation method consistent with certain embodiments of the present invention.

FIGURE 10 is a block diagram of a decoding system consistent with certain embodiments of the present invention.

FIGURE 11 is a block diagram of another decoding system consistent with certain embodiments of the present invention.

FIGURE 12 is a block diagram of another decoding system consistent with certain embodiments of the present invention.

FIGURE 13 is a flow chart of a method for providing clear packet data in a manner consistent with certain embodiments of the present invention.

DETAILED DESCRIPTION

While this invention is susceptible of embodiment in many different forms, there is shown in the drawings and will herein be described in detail specific embodiments, with the understanding that the present disclosure of such embodiments is to be considered as an example of the principles of the invention and not intended to limit the invention to the specific embodiments shown and described. In the description below, like reference numerals are used to describe the same, similar or corresponding parts in the several views of the drawings.

The terms "a" or "an", as used herein, are defined as one or more than one. The term "plurality", as used herein, is defined as two or more than two. The term "another", as used herein, is defined as at least a second or more. The terms "including" and/or "having", as used herein, are defined as comprising (i.e., open language). The term "coupled", as used herein, is defined as connected, although not necessarily directly, and not necessarily mechanically. The term "program", as used herein, is defined as a sequence of instructions designed for execution on a computer system. A "program", or "computer program", may include a subroutine, a function, a procedure, an object method, an object implementation, in an executable application, an applet, a servlet, a source code, an object code, a shared library / dynamic load library and/or other sequence of instructions designed for execution on a computer system.

The terms "scramble" and "encrypt" and variations thereof are used synonymously herein. Also, the term "television program" and similar terms can be interpreted in the normal conversational sense, as well as a meaning wherein the term means any segment of A/V content that can be displayed on a television set or similar monitor device. The term "video" is often used herein to embrace not only true visual information, but also in the conversational sense (e.g., "video tape

recorder") to embrace not only video signals but associated audio and data. The term "legacy" as used herein refers to existing technology used for existing cable and satellite systems. The exemplary embodiments disclosed herein are decoded by a television Set-Top Box (STB), but it is contemplated that such technology will soon be incorporated within television receivers of all types whether housed in a separate enclosure alone or in conjunction with recording and/or playback equipment or Conditional Access (CA) decryption module or within a television set itself. The present document generally uses the example of a "dual partial encryption" embodiment, but those skilled in the art will recognize that the present invention can be utilized to realize multiple partial encryption without departing from the invention. Partial encryption and selective encryption are used synonymously herein.

The selective encryption processes described in the above patent applications utilize any suitable encryption method. However, these encryption techniques are selectively applied to the data stream, rather than encrypting the entire data stream, using techniques described in the above-referenced patent applications. In general, but without the intent to be limiting, the selective encryption process utilizes intelligent selection of information to encrypt so that the entire program does not have to undergo dual encryption. By appropriate selection of data to encrypt, the program material can be effectively scrambled and hidden from those who desire to hack into the system and illegally recover commercial content without paying. MPEG (or similar format) data that are used to represent the audio and video data does so using a high degree of reliance on the redundancy of information from frame to frame. Certain data can be transmitted as "anchor" data representing chrominance and luminance data. That data is then often simply moved about the screen to generate subsequent frames by sending motion vectors that describe the movement of the block. Changes in the chrominance and luminance data are also encoded as changes rather than a recoding of absolute anchor data. Thus, encryption of this anchor data, for example, or other key data can effectively render the video un-viewable.

In accordance with certain embodiments consistent with the above inventions, the selected video data to be encrypted may be any individual one or combination of the following (described in greater detail in the above applications): video slice headers appearing in an active region of a video frame, data representing an active region of a video frame, data in a star pattern within the video frame, data representing scene changes, I Frame packets, packets containing motion vectors in a first P frame following an I Frame, packets having an intra_slice_flag indicator set, packets having an intra_slice indicator set, packets containing an intra_coded macroblock, data for a slice containing an intra_coded macroblock, data from a first macroblock following the video slice header,packets containing video slice headers, anchor data, and P Frame data for progressively refreshed video data, data arranged in vertical and or horizontal moat patterns on the video frame, and any other selected data that renders the video and/or audio difficult to utilize. Several such techniques as well as others are disclosed in the above-referenced patent applications, any of which (or other techniques) can be utilized with the present invention to encrypt only a portion of the content.

In order to distinguish between the two or more digital television signals encrypted using the multiple encryption algorithms in accordance with certain embodiments consistent with the above inventions, multiple packet identifiers (PIDs) are utilized. This is illustrated in the dual selectively encrypted data stream shown in **FIGURE 1** as data stream 100. Normally a single set of packet identifiers is used to identify a data stream associated with a particular television program. When a television signal or other content is encrypted under the multiple selective encryption arrangement described in the above-referenced applications, the clear content shown as packets 104 is assigned a first set of PIDs (PID A), and each set of encrypted content is assigned another set of PIDs. In this example, one set of encrypted content shown as packets 108 encrypted under a first conditional access (CA) encryption system (CA system X) may share the same PID (PID A) with the unencrypted content, but this should not be considered limiting. CA system X may, for example represent a so called "legacy" encryption system. A second set of

encrypted content shown as packets 112 is encrypted under a second CA encryption system (CA system Y) and encoded with a second PID (PID B). In this example, consecutive packets 108 and 112 contain the same content encrypted under two different CA systems.

Turning now to **FIGURE 2**, a device 120 is depicted in which a source of clear packets 124 is utilized to provide a set of clear packets from a selectively encrypted stream of packets. In this exemplary embodiment, a selectively encrypted data stream such as 100 is received as an input (e.g., through a tuner and a receiver device forming a part of a television Set-Top Box (STB) or other video receiver system. The stream of selectively encrypted data is processed by a PID filter 128 which selects, for example, the stream of data represented by values of PID equal to PID A in stream 100. In this example, the output of the PID filter 128 would have only packets identified by PID A. This stream of data having only PID A is buffered in a buffer memory 132 in certain embodiments before being provided to a packet substitution circuit 136. Packet substitution circuit 136 also receives an input from the source of clear or decrypted packets 124, which may be buffered at buffer memory 140.

In accord with certain embodiments, the source of clear or decrypted packets 124 may be a magnetic, optical or magneto-optical or semiconductor storage device, for example, a CD ROM (Compact Disc Read Only Memory) or a hard disk drive or an Flash ROM. In other embodiments, the source of clear or decrypted packets may be a remote source that streams or otherwise transmits the clear or decrypted packets over a network such as the Internet. Such packets may be transmitted over either a wideband or a dial-up connection.

In this example, the source of clear packets may be encoded with PID B or some other PID to identify the packets. Such clear or decrypted packets having PID B are provided to the packet substituter 136 where they are inserted into place in the data stream containing PID A packets by a packet inserter 144. The packets should preferably be inserted at a position adjacent the encrypted packets with PID A. Thus, at the output of packet inserter 144 a data stream similar to that of

FIGURE 1 appears except that the packets 112 having PID B are now in the clear rather than being encrypted.

From here, the stream can be converted to a clear data stream by detecting the encrypted packets with PID A at encrypted packet detector 148 and discarding those packets at 152. Since encrypted packets can contain a flag bit that indicates that the packet is encrypted, the process of detecting and discarding the encrypted packets is a simple matter of reading the encryption flag and discarding all encrypted packets. At this point, the data stream contains packets with PID A which are clear and Packets with PID B which are also clear. In order to use certain standard decoders (e.g., an MPEG decoder), such as 160, it may be desirable that all packets in a particular elementary stream have the same PID. Thus, at 156, the packets having PID B can be re-mapped to have PID A. This produces a clear data stream with all packets having PID A and all packets being unencrypted. In other embodiments, decoder 160 can be programmed to accept multiple PIDs in the same data stream. This process can be carried out in a circuit 120 without need for a decryptor since no decryption actually takes place at the device 120.

It will be appreciated by one skilled in the art upon consideration of the present teaching that other configurations of data in the selectively encrypted data stream can be decoded using the same, similar or analogous circuitry. One example of another configuration of a selectively encrypted data stream is depicted in **FIGURE 3** as data stream 200. In this exemplary embodiment, the selectively encrypted packets 108 having PID A encrypted under CA system X and the selectively encrypted packets 112 having PID B encrypted under CA system Y are combined with clear packets 204 having PID C.

In this embodiment, the data stream may be processed using the circuit 218 of **FIGURE 4**, the incoming selectively encrypted data stream can be processed by a PID re-mapping circuit 220 to convert the PID C packets to PID A (or equivalently, the PID A packets can be converted to PID B, both can be mapped to another PID,

or other mappings can be used). In this example, the re-mapped stream from 220 is then passed to a PID filter 128 that in this case is configured to throw away packets except those having PID A. Thus, the PID B packets are discarded at PID filter 128.

The packets from PID filter 128 can be buffered at a buffer memory 132 and then provided to the packet substituter 236. The source of clear or decrypted packets 124 can provide packets to a PID re-mapper 240 that re-maps the PID of the clear packets to PID A. The PID re-mapper 240's output can be buffered by buffer 140 and then provided to the packet inserter 144 of packet substituter 236. Packet inserter 144 then inserts the clear PID A packets into the data stream so that all packets now have PID A and the only remaining task is to remove the encrypted packets as before at 148 and 152 (e.g., by PID filtering). In other embodiments, equivalently, the encrypted packets can remain in place if ignored by the decoder 160.

In another embodiment, the PID re-mapper 220 of **FIGURE 4** may be omitted as can the PID filter 128. In this example, clear packets from 124 may also not require remapping at 240. In order to effect the packet substitution, the clear packets from 124 are inserted into the data stream adjacent the encrypted packets and the encrypted packets can be removed using PID filtering if the encrypted packets have different PID values from the clear packets. If not, the encrypted flag can be used to identify and delete the encrypted packets. Other variations will occur to those skilled in the art. Preferably, at the output of the packet substituter, all PIDs wind up the same when provided to the decoder 160. However, this is not an absolute requirement if the decoder can deal with multiple PID values for a single elementary data stream.

It should be clear to those skilled in the art upon consideration of this teaching that the particular PID assignments used in a particular selectively encrypted data stream as well as the PID assignments for the clear data from 120 is not particularly important as long as they can be determined in a manner that permits the desired substitution, and in some instances, remapping to a single PID

value for decoding. Thus, any suitable PID mapping can be used without departing from certain embodiments consistent with the present invention.

The various systems described above can be generically represented by the block diagram of circuit 320 of **FIGURE 5** in which a single or multiple selectively encrypted data stream is processed by a packet substituter 336 in which a source of clear packets 124 provides clear packets which are substituted for the encrypted packets in the input data stream. This produces a stream of clear packets that can be decoded by a suitable decoder 160. Thus, an apparatus for manipulating a selectively encrypted data stream in a manner consistent with certain embodiments has a filter that selects a set of packets from the selectively encrypted data stream based upon packet identifier values to produce a stream of packets having clear packets and encrypted packets. A packet substituter inserts a clear version of the encrypted packets into the stream of packets in place of the encrypted packets to produce a stream of clear data.

The above-referenced systems and processes use a source of clear packets that can be either supplied as a data stream or computer file, etc. from the original source of the content (or subsequent processor), or can be generated by decryption of selectively encrypted content. **FIGURE 6** depicts one exemplary system that can act as source 124 of the decrypted packets. In this system, the selectively encrypted data stream such as 100 is provided as an input. The system first identifies one of the two sets of encrypted packets to decrypt. In this case, this is easily accomplished using a PID B filter 350 to select the packets encrypted under the encryption process defined by conditional access system Y. (In other embodiments, packets could be selected by selecting encrypted packets with PID A.) These packets are then decrypted using CA decryption system 354 to produce a set of packets that are decrypted. This set of packets represents only one set of the encrypted packets, and thus is much smaller generally than the entire content represented by the selectively encrypted data stream. This set of packets can then be stored as a computer file on a computer readable storage medium 358 and / or

transmitted using a transmitting device such as a broadband or narrowband modem 362 to a remote location where the decoding of the selectively encrypted data stream is to take place. In some cases, the storage medium can be, for example, an optical disk or a magnetic disk or semiconductor storage device. Such devices can then either be directly distributed to an end user or used as a source for later transmission, e.g., over the Internet.

Therefore, an apparatus for supplying decrypted packets for substitution in place of encrypted packets in a selectively encrypted data stream in a manner consistent with certain embodiments has an encrypted packet detector that detects a set of encrypted packets in the selectively encrypted data stream and discards packets in the data stream that are not encrypted. A decrypter decrypts the set of encrypted packets in the selectively encrypted data stream to produce a set of decrypted clear packets, wherein the decrypted clear packets can be substituted for the encrypted packets in the selectively encrypted data stream.

In another embodiment, a file or stream of data packets 368 as depicted in **FIGURE 7** can be utilized. In this embodiment, when the decrypter 354 of **FIGURE 6** decrypts the encrypted packets, they are stored along with the encrypted packets at a position adjacent one or more of the encrypted packets. In this example, the packets 108 with PID A encrypted under CA system X are followed by a packet 112 containing identical data except encrypted under CA system Y and having PID B. These packets are then followed by a clear packet 370 containing the decrypted version of the packet's payload, which may have any selected PID (shown as PID F). This arrangement can be modified in the order of presentation of the packets or can only, for example contain one of the encrypted versions of the packets. (either 108 or 112) in other exemplary embodiments. This file or data stream can then be sent to the decoding device. In this embodiment, the selectively encrypted data stream can be easily modified by matching one or both of packets 108 and 112 to the packets in the original data stream. The placement of the clear packets

370 (in this case, immediately following the encrypted packets) identifies the packets that can be substituted for the encrypted packets.

Any of the above decoding techniques can be implemented in a television STB that has had software modifications to facilitate the operation as described. Also, the above techniques can be implemented in any suitable video player device including, but not limited to, a personal computing device or television receiver.

The basic decoding processes just described can be carried out by the process 400 shown in **FIGURE 8**.starting at 402. At 406 a selectively encrypted data stream is received and a set of clear packets is received at 410. The clear packets can be received and stored prior to receipt of the selectively encrypted data stream, or the process can occur substantially simultaneously. At 414, the clear packets are substituted for the encrypted packets in the selectively encrypted data stream to produce a clear data stream. This clear data stream can then be decoded and played at 418. The process ends at 422 after the last substitution and decoding has taken place.

Thus, a method of decoding a selectively encrypted data stream consistent with certain embodiments involves receiving the selectively encrypted data stream from a first source; receiving a set of clear packets from a second source, the set of clear packets containing data representing an unencrypted version of the encrypted packets present in the selectively data stream; detecting a plurality of encrypted packets forming a part of the selectively encrypted data stream; and substituting the clear packets for the encrypted packets to form a clear data stream.

One process described above for creation of the file or data stream containing the clear data stream is depicted as process 430 of **FIGURE 9** starting at 434. A file or data stream of the selectively encrypted content is received at 438 and is decrypted using an appropriate decrypter to produce a set of clear packets corresponding to the encrypted packets originally appearing in the selectively encrypted content at 442. This set of clear packets is then stored and/or transmitted to another decoding device at 446 and the process ends at 450.

Thus, a method of generating a set of clear packets consistent with certain embodiments involves receiving a selectively encrypted stream of data; detecting encrypted packets within the selectively encrypted stream of data; creating a set of clear packets by decrypting the encrypted packets detected within the selectively encrypted stream of data. Additionally, a method of facilitating decoding of a selectively encrypted data stream involves creating a set of clear packets corresponding to a set of encrypted packets present in the selectively encrypted data stream; and providing the set of clear packets to a decoder for substitution in place of the set of encrypted packets present in the selectively encrypted data stream.

The decoding mechanism previously described can be realized in many ways to decode programming from, for example, a cable television or satellite television network. By way of example, and not limitation, **FIGURES 10 - 12** depict several overall systems in which certain embodiments of the present invention can be utilized to decode selectively encrypted content. In **FIGURE 10**, a cable television system headend 504 transmits content that is selectively encrypted through cable network 508 to a television Set-Top Box 512 for decoding. In order to decode the content, a source of clear packets 124 corresponding to a set of the selectively encrypted packets transmits the clear packets via, for example, the Internet 516 or electronic mail to the STB 512's internal modem. The STB 512 software then implements a decoding process such as one of the exemplary processes previously described.

A similar process can be used to decode the selectively encrypted content in the system depicted in **FIGURE 11**, except that in this exemplary embodiment, the clear packets are received, e.g., by virtue of a subscription service, in the form of a computer readable storage medium such as a Compact Disc (CD) or Digital Versatile Disc (DVD) 520. In other embodiments, the clear packets could equally well be supplied in the form of semiconductor storage devices or any other suitable computer readable storage medium. The storage medium is played in a suitable

player 524 in order to access the clear packets. The clear packets are thus supplied to STB 512 which operates in a manner similar to that previously described except that the source of clera packets is different.

A similar process can be used to decode the selectively encrypted content in the system depicted in **FIGURE 12**, except that in this exemplary embodiment, the clear packets are received, e.g., by virtue of a subscription service, by any suitable mechanism and stored on a hard disc drive or similar device 530. The clear packets can be received in any manner and retrieved as needed from the disc drive 530. The clear packets are thus supplied to STB 512 which operates in a manner similar to that previously described except that the source of clear packets is different.

Thus, a data signal for use in decoding a selectively encrypted data stream, can have a collection of unencrypted data packets corresponding to a set of encrypted data packets, the encrypted data packets forming one set of selectively encrypted packets that represent an encrypted part of the selectively encrypted data stream. Another data signal can have a selectively encrypted data stream in which a set of encrypted packets have been removed and replaced by a set of decrypted packets, wherein the decrypted packets are obtained from a separate source. Either of these data signals can be transmitted or stored in a computer readable storage medium.

A subscription service can operate according to a method for decoding selectively encrypted content in a manner consistent with process 550 of **FIGURE 13** starting at 554 which involves generating a set of decrypted data packets at 558 corresponding to a set of encrypted data packets appearing in the selectively encrypted content by decryption of the set of encrypted data packets; obtaining a fee from a purchaser at 562; and delivering the set of unencrypted data packets to the purchaser at 566. The process then stops at 570.

While the above descriptions presume that a television STB is used as the playback device for a cable or satellite broadcast, this should not be considered

limiting. The playback device could equally well be equivalently built into a television receiver of any sort or may form a part of a personal computing device without limitation. Moreover, although the preferred embodiment utilizes a cable television or satellite television system as the source of selectively encrypted content, other sources such as packaged media could equivalently be decoded in this manner.

The source of clear packets can provide such clear packets as a subscription service wherein the subscriber purchases, leases or otherwise obtains a STB or personal computing device with appropriate software or installs suitable programming on a commercially available STB or other playback device. In exchange for subscription fees, the user can then obtain copies of the clear packets from the source of clear packets 124 by email or download to the STB 512, and can subsequently decode the encrypted programming.

Those skilled in the art will recognize. upon consideration of the above teachings, that certain of the above exemplary embodiments are based upon use of a programmed processor. However, the invention is not limited to such exemplary embodiments, since other embodiments could be implemented using hardware component equivalents such as special purpose hardware and/or dedicated processors which are equivalents. Similarly, general purpose computers, microprocessor based computers, micro-controllers, optical computers, analog computers, dedicated processors, application specific circuits and/or dedicated hard wired logic may be used to construct alternative equivalent embodiments.

Those skilled in the art will appreciate, upon consideration of the above teachings, that the program operations and processes and associated clear packet data used to implement certain of the embodiments described above can be implemented using streaming data as well as disc storage and other forms of computer readable storage such as for example Read Only Memory (ROM) devices, Random Access Memory (RAM) devices, network memory devices, optical storage elements, magnetic storage elements, magneto-optical storage

elements, flash memory, core memory and/or other equivalent volatile and non-volatile storage technologies without departing from certain embodiments of the present invention. Such alternative storage devices should be considered equivalents.

While the embodiments above are illustrated using a dual selectively encrypted data stream, single or multiple encrypted data streams can equally well be decoded in the manner taught.

Certain embodiments described herein, are or may be implemented using a programmed processor executing programming instructions that are broadly described above in flow chart form that can be stored on any suitable electronic or computer readable storage medium and / or can be transmitted over any suitable electronic communication medium. However, those skilled in the art will appreciate, upon consideration of the present teaching, that the processes described above can be implemented in any number of variations and in many suitable programming languages without departing from embodiments of the present invention. For example, the order of certain operations carried out can often be varied, additional operations can be added or operations can be deleted without departing from certain embodiments of the invention. Error trapping can be added and/or enhanced and variations can be made in user interface and information presentation without departing from certain embodiments of the present invention. Such variations are contemplated and considered equivalent.

While certain illustrative embodiments of the invention have been described, it is evident that many alternatives, modifications, permutations and variations will become apparent to those skilled in the art in light of the foregoing description. Accordingly, it is intended that the present invention embrace all such alternatives, modifications and variations as fall within the scope of the appended claims.

What is claimed is: